

ORACLE SOLARIS WITH TRUSTED EXTENSIONS

KEY FEATURES

Labeled security for absolute protection.

FEATURES

- Oracle Solaris with trusted extensions enhances existing Oracle Solaris security, preserves application investment, and provides for IT flexibility.
- Mandatory access control enforces policy-based access to data.
- Labeled desktops include CDE and trusted GNOME desktop environments.
- Labeled device access prevents malicious moving of data into the wrong hands.
- Labeled networking provides a secure way to scale your system to the network.

Oracle Solaris with trusted extensions is an advanced security feature integrated directly into Oracle Solaris 10. Trusted extensions implements labels to protect your data and applications based on their sensitivity level, not just on who owns or runs them. Credit card information, classified data, and personal records remain secure, and they can't be accessed by or written to unauthorized sources.

Extends Oracle Solaris Operating System Security

Oracle Solaris with trusted extensions broadens the proven Oracle Solaris 10 security model. It utilizes the user and process rights management feature in Oracle Solaris, Oracle Solaris Containers, file systems, and networking and doesn't require a new or separate kernel. Best of all, it doesn't require independent software vendors (ISVs) to requalify their applications to run them with sensitivity labels. And because it's an extension to Oracle Solaris 10 security policy, trusted extensions technology is flexible and quick to deploy. You can quickly add new applications, new users, and more, without extensive analysis of each application—and without the need to write complex, error-prone security policies that require a system reboot.

Mandatory Access Control

Oracle Solaris with trusted extensions mandatory access control (MAC) policy adds sensitivity labels to all aspects of the Oracle Solaris 10 operating system (OS). Labeled objects have an explicit relationship with each other, and an application can't usually see or access data with a different security label—applications are allowed read-only access to data, or to write to that data, if they have appropriate authorizations. The MAC policy applies to all aspects of the OS, including file, print, networking, window management, and device access, and even system administrators can't violate the policy inadvertently. User rights management provides a role-based access control mechanism for delegating administration tasks and enforcing separation of duties among administrators, security officers, auditors, and users.

Labeled Desktops

With trusted extensions, users who are authorized to view data at multiple classification levels can do so on a single desktop, with separation of information still strictly enforced. Competitors' products force users to repeatedly log out of one level to log into another level. Oracle enforces the MAC policy through two labeled desktop interfaces. Oracle Solaris 10 introduces the world's first labeled interface based on the GNOME open source desktop standard, but it also provides a trusted desktop with the CDE look and feel for customers familiar with the Trusted Solaris 8 OS. Each window is labeled with a stripe that alerts you at a glance about a document's security classification. The interface doesn't allow your users to drag and drop or copy files between windows with different security labels unless they have

authorization. Users can have multiple Web browsers, e-mail windows, or other applications open on the same desktop, each displaying just the data that application is cleared to view.

Labeled Device Access

With trusted extensions, devices on the system—including file systems, terminals, disk drives, USB thumb drives, CD-ROMs, printers, audio devices, and network interfaces—have labels associated with them. Security administrators can determine what types of data can be accessed by any given device, so sensitive information can't be written to devices that might be compromised or that might broadcast sensitive information to unauthorized users. Credit card data, banking records, and other classified documents can be labeled to prevent their transmission over the internet or from being copied to a floppy or CD.

Labeled Networking

Trusted extensions uses the CIPSO labeled-networking standard for exchanging data among multiple systems. CIPSO allows several systems to preserve label security when sharing data via NFS or other networking protocols, without requiring application modification. Trusted extensions also has the unique ability to create multilevel ports for any application, allowing you to use existing applications in a labeled security environment, while preserving existing investments in software and allowing for greater flexibility as application needs change.

Certified, Integrated, and Easy to Use

With the Oracle Solaris 10 3/05 release, Oracle has achieved Common Criteria independent security certification against the Controlled Access and Role Based Access Control Protection Profiles at Evaluation Assurance Level 4+ (CAPP & RBACPP @EAL 4+). It will achieve the same results with Oracle Solaris 10 11/06 by August 2007, and expect to complete Labeled Security Protection Profile (LSPP @EAL 4+) for Oracle Solaris 10 11/06, using Oracle Solaris with trusted extensions, by December 2007.

Because trusted extensions is a feature of Oracle Solaris 10, it runs on all hardware platforms that Oracle Solaris 10 does, including SPARC, x64, and x86 architectures. This means that your administrators can become familiar with trusted extensions naturally, as they learn and use other Oracle Solaris 10 security features. It also means that you can add new security levels, applications, and devices without the need to create long, error-prone security policy files.

Contact Us

For more information about Oracle Solaris with trusted extensions, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.



Oracle is committed to developing practices and products that help protect the environment

Copyright © 2007, 2010, Oracle and/or its affiliates. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0410

SOFTWARE. HARDWARE. COMPLETE.